skillsoft global knowledge™

FOCAL POINT - NETWORK FORENSICS AND INVESTIGATION I

Course Code: 100216

Learn how to differentiate between normal and abnormal network traffic, track the flow of packets through a network, and attribute conversations and actions taken over a network segment to specific hosts or users.

The preponderance of network traffic, particularly web traffic, was an expected outcome of the pivotal role that the Internet has come to play in our daily lives. The sheer volume of traffic and complexity of protocols creates a very diverse and everchanging landscape within which the network analyst must navigate.

Network Forensics and Investigation teaches attendees to differentiate between normal and abnormal network traffic, track the flow of packets through a network, and attribute conversations and actions taken over a network segment to specific hosts or users. This course focuses on research, filtering, and comparative analysis to identify and attribute the different types of activity on a network. Students will learn how to follow conversations across a wide range of protocols and through redirection and how to develop custom filters for non-dissected protocols. On Day 5 of the course, you will participate in a team-based capture-the-flag exercise to test your new skills.

What You'll Learn

- Create a baseline of the protocols, hosts and interactions in a network environment
- Identify anomalous network traffic using a combination of in-depth packet analysis and high-level statistical analysis
- Reconstruct event timelines and accurately correlate, or distinguish between, event threads
- Identify and extract network artifacts for further forensic analysis
- Compare observed network traffic to expected topology
- Research and analyze unknown (non-dissected) protocols
- Derive data of interest from encrypted traffic flows

Who Needs to Attend

- Network analysts seeking to develop security-related skills
- Incident responders needing to quickly address system security breaches

- Penetration testers looking to reduce their detectability
- Threat operations analysts seeking a better understanding of network intrusions
- All network administrators needing a better understanding of network security

Prerequisites

- A broad understanding of TCP/IP and associated protocols
- Knowledge of network hardware and segment types
- Previous exposure to Wireshark or other protocol analysis software is also recommended

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 3:32:55 AM